REPORT DOCUMENTATION PAGE

Form Approved OMB NO. 0704-0188

1. REPORT DATE (DD-MM-YYYY)	2. REPORT TYPE	3. DATES COVERED (From - To)
07-09-2016	Final Report	10-Jul-2015 - 9-Jul-2016

4. TITLE AND SUBTITLE
Final Report Proceedings: Cyber Science, Biometrics and Digital Forensics: Workshop on Emerging Cyber Techniques and Technologies

5a. CONTRACT NUMBER
W911NF-15-1-0293

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER
611102

6. AUTHORS
S.S. Iyengar, Jerry Miller

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAMES AND ADDRESSES
Florida International University
10555 West Flagler, EC 2441

Miami, FL 33174 -1630

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS (ES)
U.S. Army Research Office
P.O. Box 12211
Research Triangle Park, NC 27709-2211

10. SPONSOR/MONITOR'S ACRONYM(S)
ARO

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
67738-CS-CF.2

12. DISTRIBUTION AVAILIBILITY STATEMENT
Approved for Public Release; Distribution Unlimited

13. SUPPLEMENTARY NOTES
The views, opinions and/or findings contained in this report are those of the author(s) and should not contrued as an official Department of the Army position, policy or decision, unless so designated by other documentation.

14. ABSTRACT
A workshop in Emerging Cyber Techniques and Technologies was held at Florida International University's College of Engineering and Computing through the School of Computing and Information Sciences on November 20, 2015 to explore the Theme of Cyberscience, Biometrics, and Digital Forensics. Through this one-day workshop, over fifteen feature presentations were made and the group held two Panels to discuss "Cyberscience for the next decade," and "Security Constraints in cyber science." Researchers from over seventeen different universities and other organizations throughout the United States were represented. Following the formal

15. SUBJECT TERMS
cyberscience, biometrics, digital forensics, cybersecurity

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	15. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			Sundararaj Iyengar
UU	UU	UU	UU		19b. TELEPHONE NUMBER 305-348-3947

Standard Form 298 (Rev 8/98)
Prescribed by ANSI Std. Z39.18

Report Title

Final Report Proceedings: Cyber Science, Biometrics and Digital Forensics: Workshop on Emerging Cyber Techniques and Technologies

ABSTRACT

A workshop in Emerging Cyber Techniques and Technologies was held at Florida International University's College of Engineering and Computing through the School of Computing and Information Sciences on November 20, 2015 to explore the Theme of Cyberscience, Biometrics, and Digital Forensics. Through this one-day workshop, over fifteen feature presentations were made and the group held two Panels to discuss "Cyberscience for the next decade," and "Security Constraints in cyber science." Researchers from over seventeen different universities and other organizations throughout the United States were represented. Following the formal Workshop, several groups of researchers convened to continue discussions and to develop pathways forward in resolving challenges presented by the research groups. Many of these groups continued throughout the year, resulting in several significant collaborations, and subsequent research proposals for Department of Defense and the Department of Homeland Security in the areas of digital forensics, biometrics, digital signature science, and the newly emerging area known as Identity Science. This report contains the Workshop Proceedings with a Summary of the workshop presentations.

Enter List of papers submitted or published that acknowledge ARO support from the start of the project to the date of this printing. List the papers, including journal references, in the following categories:

(a) Papers published in peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in peer-reviewed journals:

(b) Papers published in non-peer-reviewed journals (N/A for none)

Received Paper

TOTAL:

Number of Papers published in non peer-reviewed journals:

(c) Presentations

Number of Presentations: 0.00

Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Non Peer-Reviewed Conference Proceeding publications (other than abstracts):

Peer-Reviewed Conference Proceeding publications (other than abstracts):

Received Paper

TOTAL:

Number of Peer-Reviewed Conference Proceeding publications (other than abstracts):

(d) Manuscripts

Received Paper

TOTAL:

Number of Manuscripts:

Books

Received Book

TOTAL:

Received	Book Chapter

TOTAL:

Patents Submitted

Patents Awarded

Awards

Graduate Students

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Post Doctorates

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Names of Faculty Supported

NAME	PERCENT_SUPPORTED	National Academy Member
S.S. Iyengar	0.03	
FTE Equivalent:	**0.03**	
Total Number:	**1**	

Names of Under Graduate students supported

NAME	PERCENT_SUPPORTED
FTE Equivalent:	
Total Number:	

Student Metrics

This section only applies to graduating undergraduates supported by this agreement in this reporting period

The number of undergraduates funded by this agreement who graduated during this period: 0.00

The number of undergraduates funded by this agreement who graduated during this period with a degree in science, mathematics, engineering, or technology fields:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and will continue to pursue a graduate or Ph.D. degree in science, mathematics, engineering, or technology fields:..... 0.00

Number of graduating undergraduates who achieved a 3.5 GPA to 4.0 (4.0 max scale):..... 0.00

Number of graduating undergraduates funded by a DoD funded Center of Excellence grant for Education, Research and Engineering:..... 0.00

The number of undergraduates funded by your agreement who graduated during this period and intend to work for the Department of Defense 0.00

The number of undergraduates funded by your agreement who graduated during this period and will receive scholarships or fellowships for further studies in science, mathematics, engineering or technology fields:..... 0.00

Names of Personnel receiving masters degrees

NAME

Total Number:

Names of personnel receiving PHDs

NAME

Total Number:

Names of other research staff

NAME PERCENT_SUPPORTED

FTE Equivalent:
Total Number:

Sub Contractors (DD882)

Inventions (DD882)

Scientific Progress

Since this grant was for a Workshop in in Emerging Cyber Techniques and Technologies with presentations and preliminary investigations in Cyberscience, Biometrics, and Digital Forensics, there were no significant theoretical or experimental advances presented. However, the workshop facilitated several follow-on investigations and leading to research proposals for DoD and DHS.

Technology Transfer

US Army Funded Workshop

"Emerging Cyber Techniques and Technologies"

Proceedings of the Workshop on: Cyberscience, Biometrics and Digital Forensics

November 20th, 2015
FIU - ECS 241

FIU | Engineering & Computing

FIU | Engineering & Computing

FLORIDA INTERNATIONAL UNIVERSITY

Welcome to
Emerging Cyber Techniques and Technologies Workshop

Hosted by:

School of Computing and Information Sciences

Florida International University

Sponsored by:

US Army

FIU

Computing & Information Sciences

Letter from Dr. S.S. Iyengar, Director and Ryder Chair School of Computing and Information Sciences Florida International University

Dear Workshop Participants and Community Members,

I would like to thank all of those who participated in our US Army funded Workshop on *Emerging Cyber Techniques and Technologies*!

Each of the speakers and participants provided a great mix of ideas and highlighted many research areas as well as its associated challenges that spurred others to undertake a greater role in resolving these issues. Information exchanges provided deeper understanding of the problems in these areas and provided an excellent foundation for future work.

The Workshop was a great success and has resulted in a variety of collaborations since we met in November 2015. For example, The University of Florida at Gainesville, and the University of Southern California through have been collaborating on a proposal led by Florida International University's School of Computing and Information Sciences, in the field of Identity Science, that promises to provide seminal work in this area.

Other collaborations have come about as a result, including work in digital and forensic sciences and through the Department of Defense and the Department of Homeland Security and other university research collaborators, and they have all been based upon discussions during and after the workshop. Many more collaborations are continuing and I congratulate you on taking up the challenge of continued research, and your resolve to provide new solutions to these and other emerging challenges.

These proceedings highlight the presentations that spurred these conversations and will continue to provide grist for research and resolution.

Best,

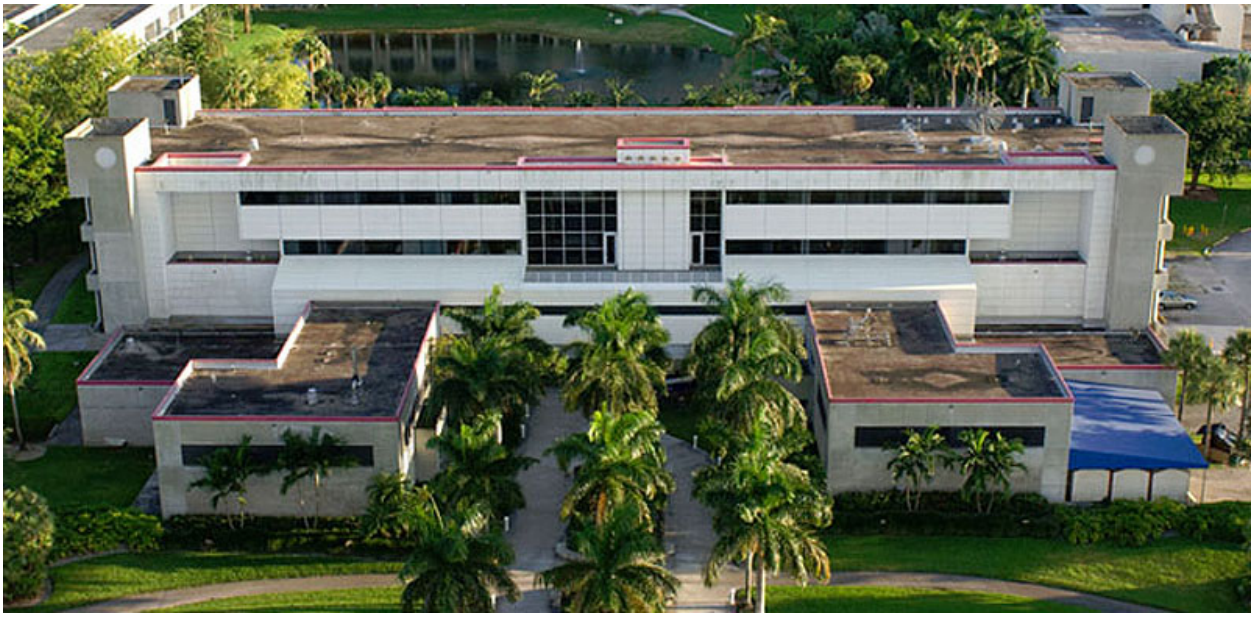
S.S. Iyengar, PhD
ACM Fellow, IEEE Fellow, AAAS Fellow, NAI Fellow
Director and Ryder Professor

Table of Contents

Welcome Letter from Dr. S.S. Iyengar

Workshop Program

Speakers Biographies and Abstracts



WELCOME

Letter from Dr. S.S. Iyengar, Director and Ryder Chair

School of Computing and Information Sciences
Florida International University

Welcome to the U.S. Army Research Office sponsored, and Florida International University hosted workshop on cyberscience, biometrics, and digital forensics! It is my great pleasure to host you at this event, and welcome you to Florida International University, South Florida's public research university.

If you are new to FIU, I'd like to provide you some facts about our university. For those of you that may not know, we are among the top 10 largest universities in the United States. We have over 55,000 students attending FIU, where 56% of our student body are women. We are number one in the nation in awarding both bachelors and masters degrees to Hispanic students. The Washington Monthly recently ranked FIU 17th among the top universities in the country, which is quite an honor. Within the School of Computing and Information Sciences, we have an outstanding, award-winning international faculty, who are passionate about teaching, research and community service.

We welcome you to this workshop, which we hope will be an excellent research opportunity for all involved. We have a variety of speakers who will be presenting work across the board in cyberscience, biometrics and digital forensics, with the goal to harness the emerging, yet disparate ideas in these cross-cutting arenas. This workshop will address five critical questions to provide new, disruptive cyberscience, biometric and digital forensic technology systems with adaptive techniques to exploit enemy, terrorists and transnational threats to our national security. We will develop an action plan to identify needs, assess vulnerabilities and address disruptive technologies that could clearly provide a decisive advantage against potential threats.

We welcome you to FIU and this workshop, and look forward to your contributions in helping us to resolve many of the computational/privacy/security challenges in cyberscience.

Thank you for participating!
Ram
S.S. Iyengar Ph.D
ACM Fellow, IEEE Fellow, AAAS Fellow, NAI Fellow
Director and Ryder Professor

PROGRAM

US Army Funded Workshop on "Emerging Cyber Techniques and Technologies"

Theme: Cyberscience, Biometrics and Digital Forensics

8:00 AM	**Registration and Networking Breakfast**
9:00 AM	**Welcome Remarks**
	President Mark Rosenberg *Provost Kenneth Furton* *Vice President of Research Andres Gil* *Dean Ranu Jung*
9:30 AM	**Introduction: US Army Research Office Overview**
	Dr. Cliff Wang U.S. Army Research Office
9:45 AM	**Keynote Talk: Biometrics Research and Operations**
	Mr. Juan Hurtado Science and Technology Advisor Deputy Director United States Southern Command Brief Q&A
10:20 AM	**Coffee Break**
10:30 AM	**Current Trends and Developments in the Forensic Sciences**
	Dr. Jose Almirall IFRI, Florida International University

11:00 AM	**Data Fusion and Real-Time Analytics for Cyber Physical Security**
	Dr. Viktor K. Prasanna CENG, University of Southern California
11:30 AM	**Biometrics Meets Hardware Security**
	Dr. Domenic Forte ECE, University of Florida
12:00 pm	**Lunch and Networking**
12:30 pm	**Quantifying Information Leakage**
	Dr. Geoff Smith SCIS, Florida International University
1:00 pm	**Integrating Biometric Sensors with Mobile Devices for Smart Services: Trends and Opportunities**
	Dr. Larry Shi CS, University of Houston
1:15 pm	**Camera Based Two-Factor Authentication for Mobile Devices**
	Dr. Bogdan Carbunar SCIS, Florida International University
1:30 pm	**Smart Grid Energy and Communication Infrastructures for Secure and Resilient Power Networks**
	Dr. Osama Mohammed ECE, Florida International University
2:00 pm	**Efficiency Privacy-Preserving Fingerprint-based Indoor Localization using Crowdsourcing**
	Dr. Kemal Akkaya ECE, Florida International University

2:30 pm	**Plausible Deniability and Her Majesty's Government. On Forensics in the Age of David Cameron.**
	Dr. Radu Sion CS, Stony Brook University
3:00 pm	**Panel 1: Cyberscience for the Next Decade**
	Dr. Charles Kamhoua (Chair) Air Force Research Laboratory *Dr. Sanjay Madria* Missouri University of Science and Technology *Dr. Xin Sun* SCIS, Florida International University *Dr. Umut Topkara* JW Player
3:30 pm	**Panel 2: Security Constraints in Cyberscience**
	Dr. Charles Kamhoua (Chair) Air Force Research Laboratory *Dr. Zhuo Lu* CS, University of Memphis *Dr. Bowei Xi* STAT, Purdue University *Dr. Zhiqiang Lin* CS, University of Texas at Dallas
4:00 pm	**Some Results on Activity and Thinking as a Biometric in Context Aware Authentication**
	Dr. Vir V. Phoha CECS, Syracuse University
4:15 pm	**Next Generation Firewalls for Strengthening Security**
	Dr. Vijay Kumar SCE, University of Missouri

4:30 pm	Game-Theoretic Solutions for Cyber Context Related Sensor Networks	
	Dr. Niki Pissinou / Dr. Charles Kamhoua SCIS, Florida International University / Air Force Research Laboratory	
5:00 pm	Cyber Security Challenges and Initiatives for Cyber Physical Systems: Smart Grid	
	Dr. Arif Sarwat ECE, Florida International University	
5:15 pm	Conference Wrap Up	
	Jerry Miller, Col., USAF (Ret) SCIS, Florida International University	
5:30 pm	Closing Remarks	
	Dr. Sitharama Iyengar SCIS, Florida International University	
5:35 pm	Reception at ECS 349	

SPEAKERS

Dr. S.S. Iyengar
Ryder Professor and Director
SCIS, Florida International University

S. S. Iyengar is a Distinguished Ryder Professor and Director of the School of Computing and Information Sciences at the Florida International University, Miami. Iyengar is a pioneer in the field of distributed sensor networks/sensor fusion, computational aspects of robotics and high performance computing. Iyengar has published over 500 research papers and has authored/edited 22 books published by MIT Press, John Wiley & Sons, Prentice Hall, CRC Press, Springer Verlag, etc. These publications have been used in major universities all over the world. His research publications are on the design and analysis of efficient algorithms, parallel computing, sensor networks, and robotics. He is also a member of the European Academy of Sciences, a Fellow of IEEE, a Fellow of ACM, a Fellow of AAAS, and a Fellow of Society of Design and Process Program (SPDS), Fellow of Institution of Engineers (FIE), awarded a Distinguished Alumnus Award of the Indian Institute of Science, Bangalore, and was awarded the IEEE Computer Society Technical Achievement for the contributions to sensor fusion algorithms, and parallel algorithms. He has received a Lifetime Achievement Award conferred by International Society of Agile Manufacturing (ISAM) in recognition of his illustrious career in teaching, research and administration and a lifelong contribution to the fields of Engineering and Computer Science at Indian Institute of Technology (BHU). Iyengar and Nulogix were awarded in the 2012 Innovation 2 Industry (i2i) Florida competition. Iyengar received Distinguished Research Award from Xaimen Uiversity, China for his research in Sensor Networks, Computer Vision and Image Processing. Iyengar's landmark contributions with his research group is the development of grid coverage for surveillance and target location in distributed sensor networks and Brooks Iyengar fusion algorithm. He has also been awarded honorary Doctorate of Science and Engineering from an institution. He serves on the advisory board of many corporations and universities in the world.He has served on many National Science Boards such as NIH - National Library of Medicine in Bioinformatics, National Science Foundation review panel, NASA Space Science, Department of Homeland Security, Office of Naval Security, and many others. His contribution was a centerpiece of this pioneering effort to develop image analysis for our science and technology and to the Goals of the US Naval Research Laboratory. The impact of his research contributions can be seen in companies/National Labs like Raytheon, Telecordia, Motorola, the United States Navy, DARPA agencies, etc. His contribution in DARPAS's program demonstration with BBN, Cambridge, Massachussetts, MURI, researchers from PSU/ARL, Duke, University of Wisconsin, UCLA, Cornell university and LSU. He is also the founding Editor of International Journal of Distributed Sensor Networks. He is presently the Editor of ACM Computing Surveys and other journals. Also he is the founding director of the FIU's Discovery Laboratory. His research work has been cited over extensively in Wikipedia and in other places. Iyengar has graduated over 45 Ph.D. students, 100s of Masters Students and large number of Post-doctoral fellows at various institutions in the world. He also had many undergraduate students working on his research projects.

His fundamental work has been transitioned into unique technologies. All through his three-decade long professional career, Iyengar has devoted and employed mathematical morphology in a unique way for quantitative understanding of computational processes for many applications.

SPEAKERS

Jerry F. Miller, Col., USAF (Ret)
Research Coordinator Discovery Lab
Florida International University

Mr. Jerry Miller is the Research Coordinator for innovation in the Discovery Lab - the undergraduate robotics and autonomous vehicles laboratory, and an Adjunct Facutly Member within the School of Computing and Information Sciences at Florida International University.

Mr. Miller is a former Associate Director at Florida International University's Applied Research Center, where he was Principal Investigator and Program Manager for three large research programs; The Western Hemisphere Information Exchange Program - conducting renewable energy, water purification and environmental sustainability research - The Western Hemisphere Security Analysis Center - an initiative designed to address the seven threats in Global Security (Human Security) - and the Strategic Culture Initiative integrating Security, Governance and Development Studies, as well as Security Technologies, into transformative and sustainable solutions.

He has authored a book on cyber security, written several book chapters, and published a variety of refereed journal articles. He has traveled, organized and presented at multiple international conferences in both Spanish and English.

Mr. Miller is a retired USAF Colonel, rescue/special operations helicopter pilot, and former USAF Foreign Area Officer with assignments in Honduras and Uruguay.

SPEAKERS

Dr. Cliff Wang
Program Manager
U.S. Army Research Office

Dr. Cliff Wang graduated from North Carolina State University with a Ph.D. in Computer Engineering in 1996. He has been carrying out research in the area of computer vision, medical imaging, high speed networks, and most recently information security. He has authored over 40 technical papers and 3 Internet standards RFCs. Dr. Wang also authored/edited for 13 books in the area of information security and holds 3 US patents on information security system development.

Since 2003, Dr. Wang has been managing extramural research portfolio on information assurance at US Army Research Office. In 2007 he was selected as the Director of the Computing Sciences Division at ARO while at the same time manages his Program in Cyber Security. For the past ten years, Dr. Wang managed over $100M research funding which resulted in significant technology breakthroughs. Dr. Wang also holds adjunct faculty position at both Department of Computer Science and Department of Electrical and Computer Engineering at North Carolina State University.

Introduction: US Army Research Office Overview

SPEAKERS

Mr. Juan Hurtado
Science and Technology Advisor Deputy Director
U.S. Southern Command Science (USSOUTHCOM)

Mr. Hurtado is the Command Science and Technology Advisor, at the United States Southern Command, Miami, Florida, where he serves as principal advisor in scientific matters and supports the Command in the formulation of material solutions to operational needs, demonstrations of technology in operational scenarios, and integration of mature technical capability into field activities in a theater of operations comprised of South and Central America and the Caribbean. Mr. Hurtado is also the Deputy Director for Technology, Innovation and Solutions, in the USSOUTHCOM J-7 Directorate. He has led the Command's technical investigations in areas such as force protection, maritime detection and monitoring, unmanned aerial systems, information technology, crisis management for disasters, peacekeeping operations, and environmental security. Prior to his current position, Mr. Hurtado culminated a career of more than 20 years commissioned service in the United States Air Force in October 2002.

He received his Master of Science degree in operations research from the Air Force Institute of Technology and his Bachelor of Science degree in Aerospace Engineering, Polytechnic University of New York. Mr. Hurtado is a member of the Acquisition Corps, and he holds acquisition certifications in Systems Planning, Research, Development and Engineering, Test and Evaluation, Program Management and Acquisition Logistics.

Keynote Talk: Biometrics Research and Operations

Biometrics is an area of interest for defense science and technology. Currently, we're investigating applications for situational awareness, crisis management, and information sharing. Our objective in present projects is to enhance the ability to register, document, monitor and reunify the missing, injured and displaced during contingencies. We're looking at biometric apps such as barcodes and facial recognition that can be employed in mobile devices in connected and disconnected environments. The technical advances in biometrics, mobile devices and apps can enhance the international response in times of crisis.

SPEAKERS

Dr. Jose Almirall
Professor and Director of IFRI
CAS, Florida International University

José R. Almirall is a Professor in the Department of Chemistry and Biochemistry and Director of the International Forensic Research Institute (IFRI) at Florida International University. He was a practicing forensic scientist at the Miami-Dade Police Department Crime Laboratory for 12 years, where he testified in over 100 criminal cases in state and federal courts prior to his academic appointment at FIU in 1998. Professor Almirall has authored one book and ~ 120 peer-reviewed scientific publications in the field of analytical and forensic chemistry and presented ~ 600 papers and workshops in the U.S., Europe, Central and South America, Australia, New Zealand, Japan and South Africa. The interests of Prof. Almirall's research group include fundamental analytical chemistry and the development of analytical chemistry tools for use in forensic science including trace detection and analysis of drugs and explosives. His research group has been awarded patents from technology developed at FIU and received ~ $ 7 million in research funding from federal agencies such as the NSF, DoD, NIJ, TSWG and from industry sources. Prof. Almirall is a Fellow of the American Academy of Forensic Sciences (AAFS), the founding chairman of the Forensic Science Education Programs Accreditation Commission (FEPAC) of the AAFS, past Chair of the FBI-sponsored Scientific Working Group on Materials (SWGMAT) Glass subgroup, a member of the editorial board of the Journal of Forensic Sciences and was appointed to serve on the Scientific Advisory Committee of the Department of Forensic Science Commonwealth of Virginia by two different governors of the State of Virginia. He was recently (2015) appointed to serve on the Forensic Science Standards Board (FSSB) of the NIST- sponsored OSAC.

Current Trends and Developments in the Forensic Sciences

The practice of forensic science is undergoing significant reform triggered by a very critical report from the National Academy of Sciences (NAS) published in 2009. The NAS highlighted the lack in scientific underpinnings in many disciplines within the forensic sciences resulting in the creation of a new National Commission on Forensic Science that will set national policy and a much broader effort that promotes the standardization of forensic science practice, the Organization of Scientific Area Committees (OSAC). A brief overview of the relevant challenges and how academic research institutes such as the International Forensic Research Institute (IFRI) at FIU are working towards meeting these challenges. The IFRI was founded in 1997 and has developed as one of the world's most recognized and productive forensic science centers with more than 8 full-time faculty devoted to forensic science research and dozens of affiliated faculty at FIU. The IFRI coordinates academic programs in forensic science at the undergraduate and graduate level and supports research faculty with access to state-of-the-art laboratory facilities. The IFRI faculty and students, as a group, publish ~ 30-35 peer-reviewed papers/year, more than any other academic institution in the U.S. and maintain active funding in several disciplines within Biology, Chemistry and Behavioral Sciences. This presentation will provide a brief overview of the research activity within IFRI and suggest some strategies to address important problems within the forensic sciences in the future.

SPEAKERS

Dr. Viktor K. Prasanna
Assistant Professor
University of Southern California

Viktor K. Prasanna (ceng.usc.edu/~prasanna) is Charles Lee Powell Chair in Engineering in the Ming Hsieh Department of Electrical Engineering and Professor of Computer Science at the University of Southern California. He is the director of the Center for Energy Informatics. He was the executive director of the USC-Infosys Center for Advanced Software Technologies (CAST) and a member of the USC-Chevron Center of Excellence for Research and Academic Training on Interactive Smart Oilfield Technologies (CiSoft). His research interests include parallel and distributed systems including networked sensor systems, embedded systems, configurable architectures and high performance computing. He served as the Editor-in-Chief of the IEEE Transactions on Computers during 2003-06 and is currently the Editor-in-Chief of the Journal of Parallel and Distributed Computing. Prasanna was the founding Chair of the IEEE Computer Society Technical Committee on Parallel Processing. He is the steering chair of the IEEE International Conference on High Performance Computing (www.hipc.org). He is a Fellow of the IEEE, the ACM and the American Association for Advancement of Science (AAAS). He is a recipient of 2009 Outstanding Engineering Alumnus Award from the Pennsylvania State University. He received the 2015 W. Wallace McDowell award from the IEEE Computer Society for his contributions to reconfigurable computing.

Data Fusion and Real-Time Analytics for Cyber Physical Security

In this presentation we will discuss two projects at USC focused on security and safety in smart infrastructures: safety in smart oil field operations and cyber physical security in smart grid. These systems consist of physical assets with human in the loop real-time control and complex cyber infrastructure. We identify three key research areas needed to build such smart systems for these domains: data fusion, real-time data access and correlative prediction. For the smart oil field project, we are developing a system for data integration so as to efficiently perform complex queries on integrated data sources. For smart grid security, we are focusing on key real time graph analytics kernels for evolving graphs.

SPEAKERS

Dr. Domenic Forte
Assistant Professor
ECE, University of Florida

Domenic Forte received the B.S. degree in Electrical Engineering from Manhattan College, Riverdale, NY, USA, in 2006, and the M.S. and Ph.D. degrees in Electrical Engineering from the University of Maryland, College Park, MD, USA, in 2010 and 2013, respectively.

Dr. Forte is currently an Assistant Professor with the Electrical and Computer Engineering Department, University of Florida, Gainesville, FL, USA, where he has been since July 2015. He is also a core faculty member of the Florida Institute for CyberSecurity (FICS). From 2013 to 2015, he was an Assistant Professor of the Department of Electrical and Computer Engineering, University of Connecticut in Storrs, CT. His research is primarily focused on the domain of hardware security and includes investigation of hardware security primitives, hardware Trojan detection and prevention, security of the electronics supply chain, and anti-reverse engineering. A secondary interest of his lies with investigation of biometrics in hardware security and the internet of things (IoT) applications.

Dr. Forte has served on the program committees of several workshops and conferences in addition to serving as session chair in many technical events. He is a co-author of the book "Counterfeit Integrated Circuits-Detection and Avoidance". He is a Guest Editor of IEEE Computer 2016 Special Issue on ``Supply Chain Security for Cyber-Infrastructure." He was a recipient of the Northrop Grumman Fellowship and the George Corcoran Memorial Outstanding Teaching Award by the Electrical and Computer Engineering Department at University of Maryland. His work has been recognized through several best paper awards and nominations, including Adaptive Hardware Systems (AHS) 2011 and Design Automation Conference (DAC) 2012.

Biometrics Meets Hardware Security

Given the number of digital systems and services we interact with every day, traditional forms of access control like passwords are becoming outmoded. Strong passwords are already difficult to remember, let alone with so many devices and services. Although dongles, smart cards, etc., are becoming more popular, their theft and misuse threaten access control. Biometrics are a more appropriate option and have several major benefits: (i) they are more convenient than passwords; (ii) if appropriately selected, they could have low probability of circumvention; (iii) they could be used to enhance the convenience and security of many applications. This presentation will cover the challenges and opportunities of biometrics in the context of new applications, such as Internet of things (IoT), and hardware security. Challenges include protection of the biometric template, privacy concerns, reliability of the authentication, and low-cost implementations. Integration of biometrics with hardware security primitives could address many of these challenges as well as emerging security concerns such as tampering and reverse engineering of systems.

SPEAKERS

Dr. Geoffrey Smith
Professor
SCIS, Florida International University

Geoffrey Smith's research interests are centered on the foundations of computer security, especially from the perspective of programming languages. For the past 20 years he has studied secure information flow, focusing first on type systems to ensure noninterference and, more recently, on quantitative information flow.

He completed his Ph.D. in Computer Science at Cornell University in 1991. Since 1994, he has been at Florida International University, where he is now a Professor in the School of Computing and Information Sciences. He has held recent visiting appointments at the École Polytechnique (France), IMDEA Software (Spain), and Macquarie University (Australia), and he is a partner in the INRIA associate team Princess and a member of IFIP Working Group 1.7. He was named an ACM Distinguished Scientist in 2013, and his 2014 paper "Additive and multiplicative notions of leakage, and their capacities" (written with Mário Alvim, Kostas Chatzikokolakis, Annabelle McIver, Carroll Morgan, and Catuscia Palamidessi) was named the winner of the NSA's third annual Best Scientific Cybersecurity Paper Competition.

Quantifying Information Leakage

A fundamental and vexing problem in cybersecurity is to prevent systems from improperly leaking the sensitive information that they process. But the problem defies simple solutions, because it is frequently necessary in practice to tolerate some leakage. Consider, for example, an election system. Individual ballots are normally considered to be confidential, but the election system needs to output the tally of votes, and this reveals some information about the individual ballots—in the case of a unanimous election, for example, this reveals how everyone voted.

For this reason, the last decade has seen growing interest in quantitative theories of information flow, which let us talk about "how much" information is leaked and perhaps allow us to tolerate "small" leaks. One major theme has been the development of leakage measures with strong operational significance, so that the amount of information leaked is associated with strong security guarantees; in this respect, notable measures include min-entropy leakage and g-leakage, which uses gain functions to model the operational scenario. A second, somewhat contrary, theme aims at robustness, trying to minimize sensitivity to (perhaps questionable) assumptions about the adversary's prior knowledge and goals. Approaches to robustness include the strong g-leakage ordering (which requires that one channel never leak more than another, regardless of the scenario) and capacity (the maximum leakage over all scenarios). This talk will survey these and other recent developments in quantitative information flow.

SPEAKERS

Dr. Larry Shi
Assistant Professor
CS, University of Houston

Mr. Shi received his Ph.D. of Computer Science from Georgia Institute of Technology. Mr. Shi was previously a senior research staff member at Motorola Research Lab, Nokia Research Center at Palo Alto, and co-founder of a technology startup focusing on value-added cloud services and infrastructure. Currently, Mr. Shi is a faculty member of the Computer Science Department at University of Houston. In the past, Mr. Shi contributed to the ASIC design of multiple NVIDIA platform products and was credited to published EA console game. In addition, Mr. Shi authored and co-authored over 70 peer-reviewed publications over a wide range of research topics. His current research efforts include identity management, security and infrastructure support for big data analytics, hardware support for security and privacy, novel biometric hardware, and cyber security issues in critical infrastructures/services. Mr. Shi was the inventor and co-inventor of multiple issued and pending USPTO patents. Mr. Shi is a senior member of IEEE. Currently, his research team is funded by National Science Foundation, Department of Homeland Security, and North Atlantic Treaty Organization.

Integrating Biometric Sensors with Mobile Devices for Smart Services: Trends and Opportunities

The rapid adoption and increasing ubiquity of mobile handheld devices enable a new biometric ecosystem that seamlessly integrates light-weight biometric sensors with mobile platform and provide great opportunities to new user-centric identity management solutions and smart services. The use of mobile biometrics increases usability and accessibility by removing spatial and temporal barriers when users control their credentials. In this talk, I will present the research results and designs on leveraging biometric sensors available on today's and future smartphones for multi-modality user authentication. These modalities support face recognition, speaker verification, fingerprint recognition, iris scan, palm recognition, and various novel behavior/soft biometrics. Such multi-modality environments enable new research opportunities for intelligent fusion and combined processing of hard and soft sources of biometric information. In addition, I will discuss emerging technologies that integrate biometric sensors, such as fingerprint sensors, directly with a touchscreen panel. The new technique transparently and continuously authenticates the mobile user during normal user-mobile device interactions and requires neither password nor extra login step. At last, I will present how the marriage of biometric sensors and mobile devices can be extended to address some of the grand challenges in physical and cyber security.

SPEAKERS

Dr. Bogdan Carbunar
Assistant Professor
SCIS, Florida International University

Bogdan Carbunar is an assistant professor in the School of Computing and Information Sciences at the Florida International University.
Previously, he held various researcher positions within the Applied Research Center at Motorola.
His research interests include distributed systems, security and applied cryptography.
He holds a Ph.D. in Computer Science from Purdue University.

Camera Based Two-Factor Authentication for Mobile Devices

The central societal role played by social media makes it an appealing fraud target, used for example as a channel for the promotion of sub-par or even malicious products, or for the distribution of misleading visual media. In this talk I will describe CaSPR lab's social media fraud detection results. First, I will present Marco and FairPlay, tools developed for Yelp and Google's Android app market, and show that they discover hundreds of fraudulent businesses and mobile apps. In addition, I will introduce Movee and Vamos, tools we developed to assert the ``liveness'' of mobile videos. I will then describe the applicability of these tools to mobile authentication, citizen journalism and smart cities.

SPEAKERS

Dr. Osama A. Mohammed

Professor and Director of the Energy Systems Research Laboratory
ECE, Florida International University

Professor Mohammed is world renowned in the power and energy systems field. He performed multiple research projects for Federal agencies and industries over the past 35 years. Most of these projects deal with energy systems, power electronics, and physics based modeling, electromagnetic signature, electric machinery and drives, high frequency switching, electromagnetic interference and smart grid modeling, analysis and operation. Professor Mohammed has currently active research programs in a number of these areas funded by DoE, DoD, NSF and several industries. Professor Mohammed has published more than 400 articles in refereed journals and other IEEE refereed International conference records. He also authored a book and several book chapters. Professor Mohammed is an elected Fellow of IEEE and is an elected Fellow of the Applied Computational Electromagnetic Society. Professor Mohammed is the recipient of the prestigious IEEE Power and Energy Society Cyril Veinott electromechanical energy conversion award and the 2012 outstanding research award from Florida International University. Professor Mohammed has lectured extensively with numerous invited and plenary talks at major research and industrial organizations worldwide. He serves as editor of several IEEE Transactions including the IEEE Transactions on Energy Conversion, the IEEE Transactions on Smart Grid, IEEE Transactions on Magnetics, IEEE Transactions on Industry Applications, COMPEL and the IEEE Power Engineering Letters. Professor Mohammed served as general chair for seven major IEEE International conferences. He also served as technical program chair for several other international conferences. Dr. Mohammed served as President of the Applied Computational Electromagnetic Society and has chaired a number of IEEE technical society committees as well as on the IEEE power and energy society governing board.
Professor Mohammed holds and MS and PhD degrees from Virginia Polytechnic Institute and State University, Blacksburg, Virginia, USA.

Smart Grid Energy and Communication Infrastructures for Secure and Resilient Power Networks

The increased penetration levels of renewables and distributed energy resources lead to increased challenges in maintaining reliable control and operation of the grid. Integrating a wide variety of systems governed by different regulations and owned by different entities to the grid increases the level of uncertainty not only on the demand side but also in terms of generation resource availability. This complicates the process of achieving generation versus demand balance. Renewable energy sources vary by nature and require intelligent forecasting and prediction systems to determine how and when this energy can be used. Controlling distributed resources that owned by customers which have enough capacity to support the grid during peak hours and provide ancillary service is another challenge. Most of these distributed resources will be installed on the distribution network, which already in its current state, lacks the proper communication and control network necessary to control the applicable resources. Moreover, the large number and widespread use of these resources makes them difficult to control from a central location.

SPEAKERS

Dr. Kemal Akkaya
Associate Professor
ECE, Florida International University

Dr. Akkaya leads the Advanced Wireless and Security Lab (ADWISE) at FIU. His research areas span various challenges of mobile and wireless networks, Internet-of-things and cyber-physical systems such as security, privacy, quality of service, topology control and mobility management. His research group design and implement algorithms that can be incorporated in real-life applications. Dr. Akkaya is the Area Editor of Elsevier Ad Hoc Networks and serves on the editorial board of IEEE Communication Surveys and Tutorials. He has been a guest editor for various journals and serves in the organizing committees of leading IEEE communication conferences such as IEEE LCN, ICC, Globecom, WCNC and SmartGridComm. He has published over 100 papers that are cited more than 6000 times so far. Dr. Akkaya is a senior member of IEEE, IEEE Computer Society and IEEE Technical Committees on Communication, Cybersecurity, Smart Cities and Online Social Networks.

Efficient Privacy-Preserving Fingerprint-based Indoor Localization using Crowdsourcing

Indoor localization has been widely studied due to the inability of GPS to function indoors. Numerous approaches have been proposed in the past and a number of these approaches are currently being used commercially.

However, little attention was paid to the privacy of the users especially in the commercial products. Malicious individuals can determine a client's daily habits and activities by simply analyzing their WiFi signals and tracking information.

In this talk, we will present the design and implementation of a privacy-preserving indoor localization scheme that is based on fingerprinting approach and analyze the performance issues in terms of accuracy, complexity, scalability and privacy.

The developed Android app which was tested on the third floor of the FIU Engineering Center provided a large data set for performance enhancements. Through analysis we will present how the performance can be improved by incorporating some techniques to the privacy-preserving localization scheme.

SPEAKERS

Dr. Radu Sion
Professor
Stony Brook University

Radu Sion is a Professor at Stony Brook University, the Director of the National Security Institute, and the CEO of Private Machines Inc.

Dr Sion's research is in Cyber Security and Large Scale Computing. He has published over 85 peer reviewed works in top venues, and has organized more than 65 conferences. Dr. Sion has received the National Science Foundation CAREER award for his work on cloud computing security.

Dr. Sion has worked with and received funding from numerous industry and government partners, including the US Air Force, the Office of the Secretary of Defense, the Department of Homeland Security, the US Army, the Intelligence ARPA, the Office of Naval Research, Northrop Grumman, IBM, NOKIA, Motorola, Xerox Parc, Microsoft, SAP, CA Technologies, the National Science Foundation, and many others.

Dr. Sion is currently leading Private Machines Inc., a cyber security startup designing the next generation secure cloud computing technologies.

Plausible Deniability and Her Majesty's Government. On Forensics in the Age of David Cameron.

Private or sensitive information is present on our disks, phones, watches and computers. Its protection is essential. Plausible deniability of stored data allows individuals to deny that their device contains a piece of sensitive information. This constitutes a key tool in the fight against oppressive governments and other sophisticated censorship tools. Further, unfortunately, recent developments in democratic, developed countries such as the UK seem to have left plausible deniability as the last available tool in the fight for privacy and personal freedom.

In this talk we will briefly discuss these and other developments and present a solution that significantly advances the state and performance of the art by an order of magnitude. Existing solutions, such as the now defunct TrueCrypt, can defend only against an adversary that can access a device at most once. Recent solutions have aimed to address this issue and ended up trading significant performance for the ability to handle powerful adversaries allowed to access a device at multiple points in time.

In this work we show that this sacrifice is not necessary. We introduce and build DataLair, a practical plausible deniability scheme, designed around a new write-only ORAM construction. DataLair is significantly more efficient than previous solutions. Reads of public, non-hidden data are as efficient as in an off-the-shelf storage and two orders of magnitude more efficient than existing approaches. Access to hidden data is also 3-5 times faster than existing approaches.

SPEAKERS

Dr. Charles Kamhoua
Research Electronics Engineer
Air Force Research Laboratory

Charles A. Kamhoua received his B.S. in Electronics from the University of Douala (ENSET), Cameroon in 1999, and the M.S. in Telecommunication and Networking and Ph.D. in Electrical Engineering from Florida International University in 2008 and 2011 respectively. In 2011, he joined the Cyber Assurance Branch of the U.S. Air Force Research Laboratory (AFRL), Rome, New York, as a National Academies Postdoctoral Fellow and became a Research Electronics Engineer in 2012. Prior to joining AFRL, he was an educator for more than 10 years. His current research interests cover the application of game theory and mechanism design to cyber security and survivability. He has over 50 technical publications in prestigious journals and International conferences including a Best Paper Award at the 2013 IEEE FOSINT-SI. Dr. Kamhoua has been recognized for his scholarship and leadership with numerous prestigious awards including the 2016 Charles E. Perry Young Alumni Visionary Award, the 2015 AFOSR Windows on the World Visiting Research Fellowship at Oxford University, the 2015 Black Engineer of the Year Award, the 2015 NSBE Golden Torch Award, and selection to the 2015 Heidelberg Laureate Forum. He is an advisor for the National Research Council, a Senior Member of IEEE and a member of ACM..

Game Theory with Learning for Cyber Security Monitoring

Recent attacks show that threats to cyber infrastructure are not only increasing in volume, but are getting more sophisticated. The attacks may comprise multiple actions that are hard to differentiate from benign activity, and therefore common detection techniques have to deal with high false positive rates. Because of the imperfect performance of automated detection techniques, responses to such attacks are highly dependent on human-driven decision-making processes. While game theory has been applied to many problems that require rational decision making, we find limitation on applying such method on security games when the defender has limited information about the opponent's strategies and payoffs. In this work, we propose Q-Learning to react automatically to the adversarial behavior of a suspicious user to secure the system. This work compares variations of Q-Learning with a traditional stochastic game. Simulation results show the possibility of Naive Q-Learning, despite restricted information on opponents.

SPEAKERS

Dr. Sanjay Madria
Professor and Associate Chair for Research
Missouri University of Science and Technology

Sanjay Kumar Madria is a full professor in the Department of Computer Science at the Missouri University of Science and Technology (formerly, University of Missouri-Rolla, USA) and site director, NSF I/UCRC center on Net-Centric Software Systems. He has published over 200 journal and conference papers in the areas of mobile data management, sensor computing, and cyber security and trust management. He won five IEEE best papers awards from conferences such as IEEE SRDS 2015, IEEE MDM 2012 and IEEE MDM 2011. His research is supported by several grants from federal sources such as NSF, DOE, AFRL, ARL, ARO, NIST and industries like Boeing, Unique*Soft, etc. He has also been awarded JSPS (Japanese Society for Promotion of Science) visiting scientist fellowship in 2006 and ASEE (American Society of Engineering Education) fellowship at AFRL from 2008 to 2015. In 2012-13, he was awarded NRC Fellowship by National Academies. He has received faculty excellence research awards in 2007, 2009, 2011 and 2013 from his university for excellence in research. He served as an IEEE Distinguished Speaker, and currently, he is an ACM Distinguished Speaker, and IEEE Senior Member and Golden Core awardee.

Panel 1: Cyberscience for the Next Decade
Secure Sensor Cloud

Traditional model of computing with wireless sensors imposes restrictions on how efficiently wireless sensors can be used due to resource constraints. Newer models for interacting with wireless sensors such as Internet of Things and Sensor Cloud aim to overcome these restrictions. In this talk, I will discuss a sensor cloud architecture where virtual sensors assist in creating a multi user environment on top of resource constrained physical wireless sensors and can help in supporting multiple applications on-demand basis. I will then present some security issues and provide overview of the solutions to the problems. In particular, I will discuss energy efficient privacy and data integrity preserving data aggregation algorithm, risk assessment in sensor cloud as well as attribute-based access control for sensor cloud applications.

SPEAKERS

Dr. Xin Sun
Assistant Professor
SCIS, Florida International University

Dr. Xin Sun received his Ph.D. in 2012 from Purdue University and B.E. in 2005 from University of Science and Technology of China, both in Computer Engineering. Since 2012 he has been an assistant professor in the School of Computing and Information Sciences at Florida International University, Miami. In 2014, he was a visiting researcher at IBM T.J. Watson Center from June to August. His research interests are in computer networks and network security, with focuses on the design and management of network access control, large scale distributed denial of service attacks, and software-defined networking. He received the NSF CRII award for young investigators in May 2015.

Panel 1: Cyber Science for the Next Decade

SPEAKERS

Dr. Umut Topkara
Research Engineer
JW Player

Umut Topkara is a research engineer with JW Player. Previously, he held research staff and engineering positions at the IBM T.J. Watson Research Lab and Google. His research interests include mobile collaboration, security, and machine learning. He holds a Ph.D. in Computer Science from Purdue University.

Panel 1: Cyberscience for the Next Decade
Pixie: Image-based Behaviormetric Authentication

JW PlayerPixie is a novel two-factor authentication solution for mobile devices. Pixie leverages behavior metrics from the images of physical objects carried, worn, or otherwise readily accessible to users, called ``trinkets'' to establish trust. Pixie combines graphical password and physical token based authentication concepts in a single familiar action of capturing a photo. We will present a user study that evaluates and compares Pixie against traditional text-based password authentication. The results show that Pixie outperforms text passwords on memorability, speed, and user preference. Pixie demonstrates a promising alternative for mobile authentication, as it is also both discoverable and accurate, and users are able to remember their trinkets hiding in plain sight even 7 days after registering them. Joint Work with: Bogdan Carbunar, FIU, Mozhgan Azimpourkivi, FIU

SPEAKERS

Dr. Zhuo Lu
Assistant Professor
CS, University of Memphis

Dr. Zhuo Lu is an Assistant Professor at the Department of Computer Science, University of Memphis. He currently leads the Communications, Security, and Analytics (CSA) Lab at University of Memphis.

He received his Ph.D. degree from North Carolina State University in 2013. He was a research scientist at Intelligent Automation Inc., Rockville MD from 2013 to 2014. Dr. Lu's research interests include cyber security, network attack modeling and analysis, proactive defense, information forensics, data analytics, cyber-physical systems, wireless and mobile systems. He is a member of ACM and IEEE.

Panel 2: Security Constraints in Cyberscience

SPEAKERS

Dr. Bowei Xi
Associate Professor
STAT, Purdue University

Bowei Xi received her Ph.D in statistics from the Department of Statistics at the University of Michigan, Ann Arbor in 2004. She is an associate professor in the Department of Statistics at Purdue University. She was a visiting faculty in the Department of Statistics at Stanford University in summer 2007, and a visiting faculty at Statistical and Applied Mathematical Sciences Institute (SAMSI) from September 2012 to May 2013. Her research focuses on multidisciplinary Work involving big datasets with complex structure from very different application areas including cyber security, Internet traffic, metabolomics, machine learning, and data mining.

She has a US patent on an automatic system configuration tool and has filed another patent application for identification of blood based metabolite biomarkers of pancreatic cancer. She also participates in the development of a novel software environment, Tessera, which allows analysts to carry out deep analysis of complex big datasets wholly within R (http://tessera.io/).

Panel 2: Security Constraints in Cyberscience

SPEAKERS

Dr. Zhiqiang Lin
Assistant Professor
CS, University of Texas at Dallas

Dr. Zhiqiang Lin is an Assistant Professor at the University of Texas at Dallas. He received his Ph.D. from the Department of Computer Science at Purdue University. Dr. Lin's research interests lie in systems and software security, with an emphasis of developing program analysis techniques and applying them to secure the OS Kernels as well as the running software. Dr. Lin is a recipient of the NSF CAREER Award, and the AFOSR Young Investigator Award.

Panel 2: Security Constraints in Cyberscience

It is well accepted that building hacking-proof software is challenging, and our software often contains exploitable vulnerabilities. Over the past few decades, numerous software solutions have been proposed to enhance the security of the systems and the software, and some of them have also been pushed to the hardware. For instance, one interesting feature recently introduced in x86 CPU is the processor tracing, which can be potentially used for control flow integrity. There are also FPGA based taint tracking. In general, the hardware solutions usually run much faster than the software ones. However, there are also some limitations such as lack of flexibility, and it may need the change of the upper layer software. In this panel, Dr. Lin would like to discuss the pros and cons the hardware level approaches, as well as the potential solutions.

SPEAKERS

Dr. Vir V. Phoha
Professor of Computer Science
CECS, Syracuse University

Dr. Vir V. Phoha is a Professor of Electrical Engineering and Computer Science in the College of Engineering and Computer Science at Syracuse University, New York. His research interest includes behavioral biometrics, machine learning, anomaly detection, spatial-temporal pattern detection and event recognition, and knowledge discovery and analysis. Professor Phoha is an ACM Distinguished Scientist and is a Fellow of SDPS.

Dr. Phoha has received research funding from DARPA, NSF, ONR, ARO, AFOSR, AFRL, and Louisiana Board of Regents among others. Professor holds 13 patents, eight of which are in behavior biometrics. His technology is licensed to major companies in biometrics. He is author of five books and over 180 research publications. Through a series of research papers, he has introduced novel secure behavioral authentication algorithms and methods that include point-in-time authentication and continuous authentication. He was the first to introduce robotic attacks and defense mechanisms on behavioral authentication systems.

Some Results on Activity and Thinking as a Biometric in Context Aware Authentication

The way a person walks, moves hands, or touches, for example swipes, or puts pressure on a mobile device while swiping is shown to have patterns that can distinguish one individual from another individual. Context of an activity matters. We present some results of using these activity patterns as a biometric. We also show that how a person holds a phone or whether a person is listening to music can affect authentication accuracy. We present some attacks and the corresponding defense(s) on authentication systems using these modalities.

We show that thinking patterns are a viable biometrics. Using Functional Near-Infrared Spectroscopy (fNIRS) which measures the light absorbed by blood and, compared to EEG, has a higher signal-to-noise ratio, and enables targeted measurements of specific brain regions, we show that fNIRS has significant promise as a biometric authentication. Based on a dataset of 50 users that we analyzed using an SVM and a Naive Bayes classifier, our experiments give EERs of 0.036 and 0.046 when using our best channel configuration. Further, we present some results on the areas of the brain which demonstrated highest discriminative power.

SPEAKERS

Dr. Vijay Kumar
Professor Computer Science Electrical Engineering
SCE, University of Missouri-Kansas City

Vijay Kumar is a professor of computer science at the University of Missouri-Kansas City, Kansas City, Missouri, USA. His research areas are Mobile Computing, Sensor Technology, Data Warehousing, Workflow, Web, and Computational Biology. His works have been funded by NSF, AFRL, and a number of industries (HP, Sprint, etc.). He has published papers in ACM TODS, IEEE TKDE, IEEE TOC, IEEE TMC, Information Systems, Data and Knowledge Engineering, and many other. He has served as program chair, general chair, and as a PC member on a number of ACM and IEEE national and international conferences and workshops. He has written five books on database systems and mobile systems. He is editor-in-chief of two refereed journals. His most recent research is in the following area: firewall security on mobile and wired networks. It is a fact that mobile (wireless) communication has become an essential information exchange platform for today's enterprise and government organizations. Their employees extensively use mobile devices to support their job activities while they are on the move. Organizations need to secure mobile devices as they secure wired devices. Today, it is common for these organizations to have multiple external mobile and wireless connections to the outside world to provide high bandwidth and tolerate connection failures. Dr. Kumar is a senior ACM member, ACM distinguished speaker and a senior IEEE member.

Next Generation Firewalls for Strengthening Security

Conventional (static) firewall approach is incapable to secure today's infrastructure (different types of organizations). Conventional firewalls are static resources (programmed statically) that filter out attacks. While being simple, such a static policy has many disadvantages and may not provide necessary protection to mobile and wired perimeters. They are unable to react to changes in its external environment, they have physical limitations and differences in trust relationships, and completeness among a non-communicating set of policies is problematic. Next generation firewalls (dynamic firewalls) that deploy multiple firewalls with automatic (no human intervention) policy and constraints updates capability is a possible solution. It should, however, be noted that for many situations a simple dynamic approach is not sufficient. We, therefore, propose dynamic firewalling with location-based filtering approach which is capable of protecting organizations from attacks that are mounted from other side of proxy and from specific "dangerous locations." We also note that a scheme that only protects static objects is inadequate for today's requirements. Our scheme, therefore, secure mobile infrastructure as well. In order to provide perimeter protection policies that react to dynamic changes (quite frequent in mobile setups) is highly desirable.

SPEAKERS

Dr. Niki Pissinou
Professor
SCIS, Florida International University

Dr. Pissinou has published over two hundred and fifty research papers in peer reviewed journals, conference proceedings and books chapters on networking, telecommunications, distributed systems, mobile computing, security and aspects of nontraditional data management including co-editing over four texts in the area of mobile and wireless networking and systems and over fourteen IEEE and ACM conference volumes. Widely cited in books and research papers, her research has been funded by NSF, DHS, NASA, DOT, DoD, state governments and industry. She has graduated over nineteen Ph.D. students who now hold positions in academia, federal government and industry. Dr. Pissinou has served as the general and technical program chair on a variety of ACM and IEEE conferences. She also served on hundreds of IEEE and ACM program committees, organizing committees, review panels, advisory boards, editorial boards etc. She has served as an editor of many journals including the IEEE Transactions on Data and Knowledge Engineering. She also has been the founder of many professional forums, including the ACM GIS. Dr. Pissinou has given keynote talks at various events and served as consultant to industry. Her achievements have been recognized by her peers, who have given her several awards and honors, including best paper awards.

Game-Theoretic Solutions for Cyber Context Related Sensor Networks

Dr. Pissinou is giving an overview on Game-Theoretic Solutions for Cyber Context Related Sensor Networks.

SPEAKERS

Dr. Arif I. Sarwat
Assistant Professor and Director of EPRAC
EPS, Florida International University

Dr. Arif I. Sarwat received his M.S. degree in Electrical and Computer Engineering from the University of Florida, Gainesville and Ph.D. in Electrical Engineering from the University of South Florida. He joined Siemens, worked in the industry for nine years executing many multi-million dollar projects. He is the co-developer of the DOE $12M funded Gateway to Power (G2P) Project. His significant work in energy storage, microgrid and DSM is demonstrated by Sustainable Electric Energy Delivery Systems in Florida. He is also the Director and Investigator of a $7.65M research initiative with FPL/NextEra Energy entitled "Energy Power Reliability And Analytic Center (EPRAC)", which conducts high-end studies on the effect of high penetration PV integration into the Smart Grid's reliability, power quality and many other aspects.

Cyber Security challenges and Initiatives for Cyber Physical Systems: Smart Grid

Securing critical infrastructure such as the power grid has emerged as a major national and global priority. The networked nature of such critical infrastructure which facilitates their effective operation renders them vulnerable to a range of attacks both in cyber and physical domains. This has been corroborated by the emergence of malicious threats, such as the Stuxnet worm, which can rapidly compromise the primary functions of Cyber-Physical Systems (CPSs). It further necessitates the development and design of techniques that focus not just on cyber but also the physical components of the smart grid, marrying the two aspects of the security solutions.

This talk will provide a brief overview of the challenges in real-time data management systems, and the different vulnerabilities, threats and attacks that can be perpetrated against CPS, and also present novel and evolutionary solutions to counter these attacks and threats in a proactive but not reactive manner, providing a predictive window for the security analysts and operators to act upon securing the system even before the attack happens. Solutions centered on Situation Awareness, Self-Sufficient Visualization, Biometric Authentication form the focus of this presentation.

NOTES

Florida International University (FIU)

Florida International University is a comprehensive university offering 340 majors in 188 degree programs in 23 colleges and schools, with innovative bachelor's, master's and doctoral programs across all disciplines including medicine, public health, law, journalism, hospitality and architecture. FIU is Carnegie-designated as both a research university with high research activity and a community-engaged university.

Located in the heart of the dynamic south Florida urban region, our multiple campuses serve over 50,000 students, placing FIU among the ten largest universities in the nation. Our annual research expenditures are in excess of $100 million and our deep commitment to engagement have made FIU the go-to-solutions center for issues ranging from local to global.

FIU leads the nation in granting bachelor's degrees, including in the STEM fields, to minority students and is first in awarding STEM master's degrees to Hispanics.

Our students, faculty and staff reflect Miami's diverse population, earning FIU the designation of Hispanic-Serving Institution.

At FIU, we are proud to be "Worlds Ahead"!

For more information about FIU, please visit http://www.fiu.edu

School of Computing and Information Sciences (SCIS)

The School of Computing and Information Sciences (SCIS) at FIU is a rapidly growing program of excellence at the University, with 30 tenure-track faculty members and over 2,000 students, including over 80 Ph.D. students.

SCIS offers B.S., M.S., and Ph.D. degrees in Computer Science, an M.S. degree in Telecommunications and Networking, an M.S. degree in Cybersecurity, and B.S., B.A., and M.S. degrees in Information Technology.

SCIS has received over $22 million in the last four years in external research funding, has six research centers/clusters with first-class computing and support infrastructure, and enjoys broad and dynamic industry and international partnerships.

For more information about FIU SCIS, please visit http://www.cis.fiu.edu.